บทที่ 1

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน เป็นที่ยอมรับกันว่าอินเทอร์เน็ตได้เข้ามามีบทบาทในชีวิตประจำวันของบุคคลทั่วไปเป็นอย่างมาก ไม่ว่าจะเป็นการสืบค้นข้อมูล การซื้อขายสินค้า การรับส่งจดหมายอิเล็กทรอนิกส์ การเล่นเกมออนไลน์ การเข้าไปเยี่ยมชมเว็บไซต์ต่างๆ เช่น เว็บไซต์ข่าว เว็บไซต์เพื่อความบันเทิง เป็นต้น ประกอบกับการปรับปรุงโครงข่ายอินเทอร์เน็ตของผู้ให้บริการรายต่างๆ เพื่อช่วยให้การรับส่งข้อมูลสามารถทำได้อย่างรวดเร็วยิ่งขึ้น และแนวโน้มของการใช้งานอินเทอร์เน็ตที่เปลี่ยนแปลงไปในลักษณะที่ให้ผู้ใช้อินเทอร์เน็ตมีส่วนร่วมในการสร้างสรรค์เนื้อหาและนำมาแบ่งปันกับผู้ใช้อินเทอร์เน็ตคนอื่นๆภายในเครือข่าย จนเกิดเป็นชุมชนออนไลน์ที่มีการดาวน์โหลดและอัพโหลดเนื้อหา รูปภาพ และวีดีโอคลิปต่างๆเป็นจำนวนมาก ปัจจัยเหล่านี้ล้วนส่งผลให้เกิดความนิยมในการใช้อินเทอร์เน็ตเพิ่มมากยิ่งขึ้น

นอกจากนี้ อินเทอร์เน็ตยังถูกใช้เป็นช่องทางในการดำเนินธุรกิจขององค์กรต่างๆ ไม่ว่าจะเป็นการซื้อขายสินค้าและการประมูลสินค้าออนไลน์ตามเว็บไซต์ต่างๆ การเรียกดูและการซื้อขายหลักทรัพย์ผ่านอินเทอร์เน็ตของตลาดหลักทรัพย์แห่งประเทศไทย การจองตั๋วเครื่องบินผ่านอินเทอร์เน็ตของสายการบินต่างๆ รวมไปถึงการให้บริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารพาณิชย์หลายๆแห่ง เป็นต้น ซึ่งในส่วนของบริการทางการเงินผ่านอินเทอร์เน็ตนั้นจะเห็นได้ว่า ธนาคารพาณิชย์ต่างๆนั้นต่างก็แข่งขันกันออกบริการทางการเงินประเภทต่างๆมาเป็นจำนวนมากเพื่อช่วยอำนวยความสะดวกให้กับลูกค้าของตน ทั้งในระดับกลุ่มบุคคลทั่วไปและระดับองค์กร ไม่ว่าจะเป็นการสอบถามยอดคงเหลือในบัญชี การโอนเงิน การชำระค่าสินค้าและบริการ การซื้อขายและแลกเปลี่ยนกองทุน เป็นต้น พร้อมๆกับการสร้างความเชื่อมั่นให้กับลูกค้าว่าการทำธุรกรรมทางการเงินผ่านอินเทอร์เน็ตผ่านธนาคารของตนนั้นมีความปลอดภัยสูงสุด

อย่างไรก็ตาม ในปัจจุบันการกระทำอาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตได้เพิ่มจำนวนขึ้นเป็นอย่างมาก ไม่ว่าจะเป็นในเรื่องของ Spam Mail หรือการส่งจดหมายอิเล็กทรอนิกส์เป็นจำนวนมากเพื่อรบกวนการทำงานของเมล์เซิร์ฟเวอร์ การทำ Phishing หรือการจารกรรมข้อมูลทางอินเทอร์เน็ต โดยการสร้างจดหมายอิเล็กทรอนิกส์หลอกลวงเพื่อสอบถามรหัสส่วนตัวหรือข้อมูลทางการเงิน ซึ่งเกิดขึ้นกับธนาคารพาณิชย์หลายๆแห่ง การส่งไวรัสหรือหนอนอินเทอร์เน็ตเพื่อรบกวนการทำงานของระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต การโจมตีระบบเครือข่ายจนกระทั่งทำให้ระบบไม่สามารถให้บริการได้ การส่งโปรแกรมประเภท Keylogger เพื่อลักลอบดูการทำงานของเครื่องคอมพิวเตอร์ รวมไปถึงการปล่อยข่าวลวง (Hoax) และการตัดต่อภาพลามกอนาจารของคนอื่นเพื่อนำไปเผยแพร่ตามเว็บไซต์ต่างๆ เป็นต้น

อาชญากรรมดังกล่าวได้ส่งผลกระทบอย่างร้ายแรงต่อทั้งบุคคลทั่วไปที่ใช้คอมพิวเตอร์และอินเทอร์เน็ตไปจนถึงองค์กรต่างๆที่ใช้อินเทอร์เน็ตเป็นช่องทางในการดำเนินธุรกิจ โดยเฉพาะอย่างยิ่งธนาคารพาณิชย์ต่างๆ เนื่องจากธนาคารพาณิชย์เป็นองค์กรที่ดำเนินธุรกิจที่เกี่ยวข้องกับเงินและคนเป็นจำนวนมาก ดังเช่นในเรื่องของการส่งจดหมายอิเล็กทรอนิกส์หลอกลวงเพื่อสอบถามรหัสส่วนตัวและหมายเลขบัตรเครดิตจากลูกค้าโดยแอบอ้างว่าเป็นจดหมายอิเล็กทรอนิกส์ที่ส่งมาจากธนาคาร หรือการติดอุปกรณ์บางอย่างที่ตู้กดเงินอัตโนมัติของธนาคารเพื่อทำการคัดลอกหมายเลขบัตรเอทีเอ็มและรหัสส่วนตัวเพื่อนำไปใช้ทำบัตรเอทีเอ็มปลอม เป็นต้น ในขณะที่ทางภาครัฐเองก็ได้มีความพยายามที่จะป้องกันและแก้ไขปัญหาดังกล่าว ด้วยการออกร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ โดยการพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา ซึ่งมีใจความสำคัญในการกำหนดบทลงโทษผู้กระทำความผิด หลักเกณฑ์ในการเก็บข้อมูลจราจร (Traffic Data) ของผู้ให้บริการ และการกำหนดอำนาจหน้าที่ในการจับกุมผู้กระทำความผิดของเจ้าพนักงานของรัฐ เป็นต้น ซึ่งร่างพระราชบัญญัติดังกล่าวก็ได้มีการพิจารณากันมาอย่างยาวนานเป็นระยะเวลาหลายปี จนในที่สุดก็ได้เปลี่ยนชื่อเป็น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และมีผลบังคับใช้แล้วในปัจจุบัน

จากการที่อาชญากรรมทางคอมพิวเตอร์และอินเทอร์เน็ตได้เพิ่มจำนวนขึ้นเป็นอย่างมาก อีกทั้งยังมีความซับซ้อนมากขึ้น ประกอบกับการบังคับใช้พระราชบัญญัติดังกล่าวของภาครัฐส่งผลให้องค์กรต่างๆโดยเฉพาะอย่างยิ่งธนาคารพาณิชย์จำเป็นต้องปรับตัวและทบทวน

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของตนเองใหม่ โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ต ไม่ว่าจะเป็นการเพิ่มระดับของการรักษาความปลอดภัยในการเข้าใช้งานระบบให้กับลูกค้า การติดตั้งอุปกรณ์ตรวจจับความผิดปกติที่เกิดขึ้นกับระบบการให้บริการ หรือการให้ความรู้ทางด้านความปลอดภัยข้อมูลสารสนเทศแก่พนักงานอย่างเพียงพอ เพื่อให้สอดคล้องกับมาตรฐานสากลที่เป็นที่ยอมรับและข้อบังคับที่ได้ประกาศไว้ในพระราชบัญญัติดังกล่าว และยังเป็นการสร้างความน่าเชื่อถือให้แก่องค์กรและสร้างความมั่นใจให้แก่ลูกค้าของตน ทั้งนี้ การวางนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่ดี นอกจากจะเป็นการป้องกันไม่ให้ภัยคุกคามที่ไม่พึงประสงค์เกิดขึ้นกับองค์กรแล้ว นโยบายที่ดียังจะช่วยให้องค์กรสามารถเตรียมพร้อมรับมือกับภัยคุกคามไม่คาดฝันที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพอีกด้วย

วัตถุประสงค์ของงานวิจัย

1. เพื่อศึกษามาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากล 2 แบบ ได้แก่ มาตรฐาน ISO/IEC 17799:2005 และมาตรฐาน ISO/IEC 27001:2005
2. เพื่อวิเคราะห์เปรียบเทียบนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตของธนาคารที่ใช้เป็นกรณีศึกษาในปัจจุบันกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากลทั้ง 2 แบบ
3. เพื่อเสนอแนะนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตที่เหมาะสมและสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากลสำหรับธนาคารที่ใช้เป็นกรณีศึกษา

ขอบเขตของงานวิจัย

การศึกษาครั้งนี้เน้นไปที่การศึกษานโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศภายในฝ่ายเทคโนโลยีของธนาคารที่ใช้เป็นกรณีศึกษา เฉพาะในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตเท่านั้น โดยจะทำการศึกษาเปรียบเทียบกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศ 2 แบบ ได้แก่ มาตรฐาน ISO/IEC 17799:2005 และมาตรฐาน

ISO/IEC 27001:2005 เนื่องจากมาตรฐานแรกเป็นมาตรฐานที่ประกอบไปด้วยข้อกำหนดต่างๆที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่องค์กรสามารถนำมาปรับใช้ได้จริง ในขณะที่มาตรฐานหลังเป็นมาตรฐานที่เกี่ยวข้องกับแนวทางในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Management Systems: ISMS) สำหรับองค์กรเพื่อให้พร้อมรับการตรวจสอบจากผู้ตรวจสอบระบบ และการยื่นขอใบรับรอง (Certificate) ให้กับระบบของตน

ในขณะที่แนวทางหรือกรอบปฏิบัติอื่นๆที่เกี่ยวข้องกับระบบสารสนเทศภายในองค์กร เช่น COBIT (Control Objectives for Information and Related Technology) ซึ่งเป็นกรอบแนวทางของธรรมาภิบาลทางด้านเทคโนโลยีสารสนเทศ (IT Governance) ที่กล่าวถึงการตรวจสอบภายในและการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศภายในองค์กรรวมทั้งแนวทางในการจัดการความเสี่ยงอย่างเหมาะสม ITIL (IT Infrastructure Library) ซึ่งกล่าวถึงแนวทางในการบริหารจัดการและการปรับปรุงประสิทธิภาพของการให้บริการทางด้านเทคโนโลยีสารสนเทศสำหรับองค์กร หรือ CMMI (Capability Maturity Model Integration) ซึ่งเป็นมาตรฐานที่ใช้ในการปรับปรุงกระบวนการพัฒนาซอฟท์แวร์ให้มีประสิทธิภาพมากขึ้น แนวทางเหล่านี้ไม่ได้กล่าวถึงบริบทของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศภายในองค์กรอย่างชัดเจน จึงไม่ได้ถูกรวมไว้ในการศึกษาครั้งนี้แต่อย่างใด

ข้อจำกัดของงานวิจัย

การศึกษาครั้งนี้เป็นเพียงข้อเสนอแนะนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เหมาะสมสำหรับธนาคารที่ใช้เป็นกรณีศึกษา ในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตเท่านั้น จึงมีข้อจำกัดในเรื่องของการวัดผลสำเร็จของการนำข้อเสนอแนะนโยบายดังกล่าวไปปฏิบัติจริง

แผนงานวิจัย

การศึกษาครั้งนี้ไม่เสียค่าใช้จ่ายในการดำเนินการและมีระยะเวลาในการดำเนินการทั้งสิ้น 5 เดือน โดยมีขั้นตอนการดำเนินการดังต่อไปนี้

ขั้นตอนการดำเนินการ	ระยะเวลา									
	ต.ค. 51		พ.ย. 51		ธ.ค. 51		ม.ค. 51		ก.พ. 52	
1. สัมภาษณ์ Security Management Team										
2. สัมภาษณ์บุคลากรในโครงการ Internet Banking										
3. ทำเอกสารสรุปเพื่อให้ผู้ถูกสัมภาษณ์ตรวจสอบความถูกต้อง										
4. วิเคราะห์ปัญหาและจัดทำเป็นเอกสาร										
5. ศึกษามาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศ 2 แบบ										
6. วิเคราะห์ เปรียบเทียบ และจัดทำเป็นเอกสาร										
7. ทำ Gap Analysis										
8. ร่างข้อเสนอแนะนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ										
9. นำเสนอผู้บริหาร										

ประโยชน์ที่คาดว่าจะได้รับ

1. เพื่อให้ผู้ที่สนใจได้ทราบถึงมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากล 2 แบบ ได้แก่ มาตรฐาน ISO/IEC 17799:2005 และมาตรฐาน ISO/IEC 27001:2005

2. เพื่อให้ผู้ที่สนใจใช้เป็นกรณีศึกษาในเรื่องของการวางนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตสำหรับองค์กรของตน

3. เพื่อให้ธนาคารที่ใช้เป็นกรณีศึกษาได้รับทราบข้อเสนอแนะนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในส่วนที่เกี่ยวข้องกับบริการทางการเงินผ่านอินเทอร์เน็ตที่เหมาะสมและสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยด้านสารสนเทศที่เป็นมาตรฐานสากล

นิยามและคำจำกัดความที่สำคัญ

“เทคโนโลยีสารสนเทศ (Information Technology)” หมายถึง เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้น

สารสนเทศ โดยมีองค์ประกอบ 3 ส่วนคือ คอมพิวเตอร์ การสื่อสารและสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

“ความลับ (Confidentiality)” หมายถึง การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิ์เท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

“บูรณภาพ (Integrity)” หมายถึง การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ์ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

“ความพร้อมใช้งาน (Availability)” หมายถึง การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

“การพิสูจน์ฝ่าย (Authentication)” หมายถึง การตรวจสอบและการพิสูจน์สิทธิ์ของการขอเข้าใช้ระบบของผู้ใช้บริการจากรายชื่อผู้มีสิทธิ์ สำหรับอุปกรณ์คอมพิวเตอร์ รวมถึงแอพพลิเคชั่นทั้งหลาย

“การพิสูจน์สิทธิ์ (Authorization)” หมายถึง การตรวจสอบว่าบุคคล อุปกรณ์คอมพิวเตอร์ หรือแอพพลิเคชั่นนั้นๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

“การเก็บสำรองข้อมูล (Data Backup)” หมายถึง ในระหว่างการเก็บสำรองข้อมูลสำเนาของชุดข้อมูลปัจจุบันจะถูกสร้างขึ้นมา เพื่อป้องกันการสูญหาย

“การปกป้องข้อมูล (Data Protection)” หมายถึง การป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม

“การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)” หมายถึง การป้องกันข้อมูลในบริบทของ การรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทนการรักษาความมั่นคงปลอดภัยของสารสนเทศได้

“การประเมินความเสี่ยงหรือการวิเคราะห์ความเสี่ยง (Risk Assessment or Risk Analysis) ของระบบสารสนเทศ” หมายถึง การตรวจสอบโอกาสของผลลัพธ์ใดๆที่ไม่พึงประสงค์ต่อระบบสารสนเทศและผลเสียที่อาจจะเกิดขึ้นตามมาได้

“นโยบายด้านความมั่นคงปลอดภัย (Security Policy)” หมายถึง นโยบายที่แสดงเป้าหมายที่จะต้องปกป้อง และขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัย ในบริบทของความต้องการอย่างเป็นทางการขององค์กร